REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Double Patenting Rejections

Claims 1-9 were rejected under 35 U.S.C. 101 for claiming the same invention as claims 1-9 of prior U.S. Patent No. 6,279,110 ('110), and claims 10-11 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 10-11 of the '110 patent.

Accordingly, claims 1-11 have been cancelled and a new set of claims 12-21 have been added, which are not co-extensive in scope with the claims issued in U.S. Patent No. 6,279,110, and thus comply with 35 U.S.C. 101. The claims submitted in this response are also believed to be patentable with respect to the claims of the '110 patent, and thus comply with the judicially created doctrine of obviousness-type double patenting.

Claim Rejections

Claims 1 and 7 were rejected under 35 U.S.C. 112 for insufficient antecedent basis for the expression "said long term private key". Claims 1 and 7 have been cancelled in this amendment, therefore this rejection is moot.

Claims 1-11 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,880 to Sudia in view of Koyama et al. article entitled "New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n". Claims 1-11 have been cancelled in this amendment, thus rendering this rejection moot, however, the Applicant will discuss the cited prior art with respect to the new claims 12-22.

The newly added claims are directed to a method for verifying a signature for a message

m. The signature is verified using a component pair that is derived from a masked signature. Claim 1 comprises the steps of having a verifier: obtain a pair of signature components $(\bar{s}, r)$, the component $\bar{s}$ being derived from a masked signature generated by a signor; recovering a coordinate pair (x_1, y_1) using the pair $(\bar{s}, r)$ and the message m; calculate a signature component r' from one of the coordinate pairs; and verify the signature if $r' = r$. Support for this method can be found in the description at page 7, lines 2-13 and is depicted by the flowchart shown in Figure 2. The Applicant notes that the Summary of the Invention has been amended in accordance with the scope of claim 12.

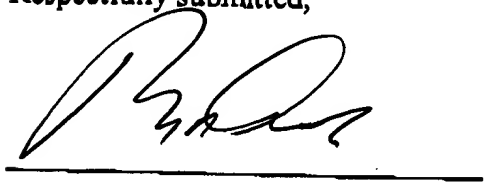
Sudia teaches a multi-step signing system using multiple signing devices to affix a single signature which can be verified using a single public verification key. Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. Sudia does not teach verifying a signature of a message using a signature component derived from a masked signature. Moreover, Sudia does not teach calculating a coordinate pair from the signature pair and using this coordinate pair to calculate a verifier signature component, i.e. r' in claim 12.

Koyama teaches various trapdoor one-way functions based on elliptic curves over the ring Z_n. Koyama also does not teach verifying a signature of a message using a signature component derived from a masked signature. Koyama also does not teach calculating a coordinate pair and using such a coordinate pair to create a verifier signature component as taught in claim 12.

Therefore, neither Sudia nor Koyama, alone or in combination, teach the method of verifying a signature as recited in claim 12. Neither reference teaches the verification steps required by claim 12, and as such, claim 12 is believed to patentably distinguish over Sudia and Koyama, and the combination thereof. Claims 13-22 are either directly or indirectly dependent on claim 12, and therefore, are also believed to distinguish over the prior art cited. Accordingly Applicant believes claims 12-22 submitted in this response are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Ralph A. Dowell
Agent for Applicant
Registration 26,868

Date: June 20, 2005

Dowell & Dowell, P.C.
Suite 406
2111 Eisenhower Avenue
Alexandria, VA 22314
USA

Tel: (703) 415-2555

21420351.1